Autorisations-, Bestimmungs-, Bezeichnungs-, Ortungs-, Verrielungs- und Diebstahl-Sicherheits-System (hier auch Lock-Loop DSS genannt)

Beschreibung

Die Erfindung betrifft eine mit keinem, einem oder mehreren Schlössern oder Algorithmen verriegelbare und/oder verschlüsselbare Öse oder mehrere Ösen. N.B. auch Mikrochips sind mit deren Transistoren verschliessbare Strom-Schalt-Kreisen, wobei der Transistor das verriegelnde Schloss und der Stromkreis die Öse ist. Jede Öse und jedes Schlösschen trägt (als zusammengehörende Einheit) eine im Internet oder auf einem Mobile-Phone-Portal oder einer anderen Datenbank registrierte Nummer oder mehrere Nummern, die Indices und Funktionen haben und die Nummer kann beliebig an Produkte befestigt werden oder gar in diesen integriert sein und einen oder mehrere Sender, Transponder oder GSM-SIM-Karten-Chips als Funk-Interface tragen bzw. in diesen integriert sein, die ein mögliches verschlüsseltes Signal auf die im Internet oder dem Mobile-Phone-Portal oder dergleichen registrierte Nummer gibt/empfängt und Alarm (bei Zerstörung, Diebstahl, Entwendung oder dergleichen) auslöst als auch den Ort der Öse lokalisiert, welche aber auch mit anderen mobilen wie stationären Funk-Sende/Empfangseinheiten lokalisiert werden kann.

Die erste Stufe der Sicherheits-Lösung ist eine rein mechanische visuelle, ob die Nummer nicht zerstört ist. Für Polizisten, Garageristen und Wiederkäufer ist dies die einfachste Methode, den rechtmässigen Besitzer eines Fahrzeuges (über das Internet) zu eruieren. Autofahrer mit zerstörter oder gar fehlender Nummer sollten gar nicht mehr möglich sein, aber diese würden mit fehlender Nummer in einem sehr grossen Erklärungsnotstand stehen nur schon wegen dieser zweiten Sicherheits-Stufe.

Die zweite Stufe der Sicherheits-Lösung ist, dass bei Zerstörung und Unterbruch der Öese, sofort immer ein Alarm über die Internet Nummer auf ein Mobil-Telefon oder eine Polizei-Zentrale etc. geht.

Ein mit diesem Autorisations-, Bestimmungs-, Bezeichnungs-, Autorisations-, Ortungs-, Verrielungs- und Diebstahl-Sicherheits-System ausgestattetes Produkt ist jederzeit durch die verschiedenen GSM-, GPS-, W-LAN- etc. Netzabdeckungen

lokalisierbar. Ein Fahrzeug oder sonstiges Produkt kann nicht mehr verschoben werden ohne Autorisation (des Besitzers) Autoschlüssel sind nicht mehr notwendig oder entwendbar, weil über das Mobil-Telefon mit einem Code oder Fingerprint der Besitzer das Fahrzeug öffnen und starten oder jederzeit abstellen und verriegeln kann.

Diese Merkmals-Kombination einer mit mehreren einem oder keinem Schloss, Riegeln, Barrieren (absichtlich selber wie auch unabsichtlich) verriegelbaren Öse, Hut, Kappe Kugel oder Box, welche eine im Internet oder auf einem Mobile-Phone-Portal registrierbare (zeitliche, veränderbare oder codierte) Auto-Nummer bzw. ein numerischer, alphanumerischer oder Barcode trägt, der bei Diebstahl oder kriminellem Gewalt-Einfluss zerstört wird und/oder bei einem anderen physikalischen sensorischen Einfluss nur schon einen Alarm auslöst, kann auch für oder an Ketten oder Schlösschen selber, (Motor-) Fahrräder (über die Speichen, Naben, Wechsler etc.), Kick-Bords, Autos, Boote, Flugzeuge, Immobilien oder Koffer, Kassetten, Mobil-Telefone, Computer, Laptops, TV, Beamer, (Elektro-) Geräte als auch jedes Kabel, oder (Faustfeuer-) Waffen, Uhren, Kleider, (Keuschheits)-Gürtel und natürlich Menschen, Tiere (Gebeine), Pflanzen wie auch Schrauben, Muttern, Nägel, Nadeln, Fäden, Knöpfe, Verpackungen, Gehäuse, Ski-Bindungen verwendet oder angebracht werden und mit einem elektrischen Stromkreis mit Anschluss oder Unterbruch zu elektrischen (Schalt)-Geräten ausgestattet sein und kann auch einen Sender bzw. Chip tragen, der ein (verschlüsseltes) Signal auf die im Internet oder auf dem Mobile-Phone-Portal oder anderen Datenbank registrierte Nummer gibt. Die Anordnung der Nummer, des Schlosses und der Ösen als auch Senders und Chips kann so leicht gebaut und gestaltet werden, dass sie zwar ohne Beschädigung auf Jahre hinaus funktionieren, aber bei geringfügigen Verletzungen zerstört werden bzw. eine andere Funktion haben, wie z.B. dass ein Alarm los geht. Die Öse, die Nummer, der elektrische Schaltkreis kann so auch eine Einheit mit der Nummer als z.B. einem Zifferblatt bilden. Das Schloss/Öse kann selber eine solche Einheit bilden, wie jede andere Anordnung mit einer Öse z.B. eine Schraube, Muttern, Nägel, Nadeln, Fäden, Knöpfe, Stift, Niete, Ring, Platte, Kugel oder Box mit Öse und Nummer. Im Fall der Kugel oder Box kann diese noch zusätzlich mit einem normalen Schlüssel-System mit oder ohne Funkübermittlung verriegelt werden. Aus der Kugel oder Box

dann Kabel als Ösen, welche innerhalb von der Kugel oder Box einen geschützten Transmitter/Transponder bzw. Sender besitzt.

Das ursprüngliche Prinzip des verriegelbaren Ösen-Internet-Nummern Patentes ist analog aus der bekannten Anmeldung für Sicherheitsbindungen WO 02/062 432 Diese Patentanmeldung beschreibt: „Einen Dreh-Klapphebel der nach der richtigen Befestigung über eine vorstehende Öse 37 des Einspannteils 15 geklappt und mittels eines (in Figur 23 dargestellten) Schlösschens 100 verriegelt wird. Mit dem Schlösschen kann verhindert werden, dass der voneinander getrennte Einspannteil und Klemmteil wieder zusammengebracht werden können. Damit hat man eine ausgezeichnete mechanische Diebstahlsicherung. Auf der Öse und an einer gut sichtbaren Stelle auf dem Sicherheits-Bindungs Interface ist zusätzlich ein numerischer, alphanumerischer oder Barcode 39 angebracht, der in einer Liste 40 des Herstellers im Internet registriert ist und wo dem durch den Kauf rechtlich anerkannte Besitzer die Möglichkeit eingeräumt wird, mit seinen Namen sein Eigentum sich selber zu schützen bzw. schützen zu lassen. Damit lassen sich gestohlene Sicherheitsbindungs Interfaces schnell eruieren, da die gute sichtbare Öse und der zugehörige Code beim gewaltsamen Entfernen des Schlösschens zerstört werden. Somit können unter anderem bei einem Unfall Sanktionen durch die Versicherungsgesellschaften ergriffen werden, weil spätestens diese Versicherungsgesellschaften jeden neuen Unfall mit dem Interface in einer Statistik ausgewiesen haben wollen und wir nur bereit sind, eingetragene Verunfallte als wirklich Verunfallte zu akzeptieren, weil sonst jeder Snowboard Unfall im Zusammenhang mit dem neuen Interface in der Statistik ausgewiesen werden könnte, was falsch wäre. Damit lassen sich auch sehr einfach und gut Asien oder Ost-Block-Imitationen verhindern.

Münzen, Geldscheine und Kreditkarten können ebenfalls mit einer (verriegelbaren) Öse, einem Microchip, oder Transponder ausgestattet werden und mit zusätzlichen Informationen über Zeit, Ort, Vergangenheit, Besitzer gespeichert werden. Auf der Kreditkarte sind alle persönlichen Daten abrufbar. Bei Zerstörung der Münzen Geldscheine oder Kreditkarten können in einem Fall der ungewollten Zerstörung die Daten und Werte zurückgebracht werden oder im Fall der kriminellen Zerstörung werden die Daten und Werte blockiert bis zur offiziellen Abklärung. Die Münzen

PAGE INTENTIONALLY LEFT BLANK

Erklärung zur Neuheit bzw. zum Stand der Technik

Bitte nehmen Sie zuerst (nochmals) davon Kenntnis, das zwischen dem Lock-Loop-(Verriegelung) und nur dem Funk-Feature ein ziemlich grosser Unterschied besteht. Das LL-Feature baut weiter auf dem Funk-Feature (zur Nummer im Internet) auf. Beide sind erfinderisch als auch neu, was hier aufgezeigt wird. Ich meine, alle neuen Produkte -auch nur mit Funk-Feature und einer Nummer im Internet- verletzen meine Anmeldung, wie eben Laptops, anhand denen ich für Handys etc. und auch EPC-Tags die Beweis-Erklärung führe. Jedenfalls sicher jedes selber verriegelbare Produkt mit Nummer im Internet fällt unter diese Patentanmeldung.

Aprops Laptops. Die haben zwar die selbe Funktion und das selbe Feature (und die selben Moleküle) wie Handys und Chips, aber dass eine solche Signal-Uebermittlung (einer örtlichen etc. Verriegelung oder Abschaltung etc.) dann auch bei Centrino Laptops gemacht werden kann, habe ich zwar nicht direkt alleine nur dafür erfunden, aber mir zuvor ja allgemein patentrechtlich schützen lassen für Laptops, Bindungen, Fahrzeuge etc.... Handys hatten noch nie das (LL-) Funk-Feature zum selber ein Verriegelung-Signal zu übermitteln, geschweige dann selber zu tracken und bei Laptops etc. gab es das auch noch nicht und jetzt haben sie es (Centrino und Theft Guard Software im BIOS), wie ich es mir beansprucht habe und es ist dort neu. Das (LL-) Funk-Feature ist neu und es ist neu mit Laptops und mit aktuellen (WAP-) Handys gibt es eine solche (selbst gewollte Verriegelung und dann Tracking) Signal-Uebermittlung noch gar nicht aber wird wohl bald (von uns) auch neu kommen. Ein Patent beansprucht ja das Neue! Ich fände es eine impertinente Anmassung eines Laptop-Herstellers, wenn er behauptete, dass das (LL-) Funk-Feature bei Laptops Stand der Technik sei. Es ist und bleibt neu, auch wenn es mit den selben Molekülen, Frequenzen und Features wie bei Handys funktioniert und mit einem "Theft Guard" erst die beste Anwendung bekommt. Ueberall wie ich es formuliert hatte, ist es neu und erfinderisch wie bei Centrino Laptops. Hmm.

Ich könnte sonst (auch noch) den Anspruch formulieren: (LL-) Funk-Feature mit/über UMTS bzw. 4. Mobilfunkgeneration. -Das gibt es ja noch nicht. Nein doch schon, weil es Frequenzen sind, die Stand der Technik sind, wie Moleküle. Also, was kann man dann überhaupt noch patentieren, wenn alles aus Molekülen und Wellen besteht? Nichts. -Nein es muss bzw. per Definition kann alles (jede Merkmalskombination), was neu und erfinderisch und gewerbsmässig ist, patentiert werden. Lock-Loops mit Nummern bei Centrino Laptops, die ein Signal auf eine Internet-Nummer geben sind neu! Aber auch bei Handys der 4. MFG! Und alle verriegelbaren (aber nicht nicht verriegelbare) trackbaren aktuellen Handys wie auch EPC-Tags gehören dazu!

Insbesondere auch meine neue kleine Mini-Erfindung, der Handys der 4. MFG mit dem LL-Feature zu beanspruchen, ist absolut gültig, weil ich in meiner Anmeldung auch für elektrische Geräte, wie Computer und Handys das LL-Feature beanspruchte. D.h. wirklich auch alle neuen Produkte mit LL-Feature fallen in meinen Patentschutzbereich. Nicht umhin hatte ich schon mit IBM und Swisscom Mobile genau deswegen Kontakt aufgenommen. Ich muss noch nicht einmal mehr ein Handy Hersteller für andere neue Folge-Generationen-Entwicklungen fragen und mit diesen eine Beteiligung

für deren Auskünfte vergeben, weil einfach alle neue Produkte, als sogar auch Produkt Generationen über eine andere Technologie wieder in meinen Patentschutzbereich hineinfallen. Das füge ich hier sicher auch noch so als Erklärung zu meinem Ösen-Internet-Nummer Patent an.

Neben WAP-Handys könnten noch elektronische Fussfesseln für den Heim-Strafvollzug die Neuheit von der verriegelbaren Öse mit Nummer im Internet niederschmettern. Aber diese Fussfesseln haben kaum eine Nummer auch auf sich selber, wie bei den Ösen bzw. Laptops oder Fahrrad- und Fahrzeug-Stand-Alone Devices zur Kontrolle und v.a. Abschreckung eines Diebstahls. Und sowieso kann man diese elektronische Fussfesseln auch nicht mit einer Funk-Device selber ver- wie v.a. entriegeln. Die sind das pure Gegenteil. Nur Fremde bzw. Autorisierte können sie entriegeln (ohne Alarmauslösung).

Mir ist es nun völlig logisch, nachvollziehbar als auch nicht von mir ungerecht, für neue Laptops mit W-LAN Feature als auch genau gleich für neue Handys der 4. MFG oder auch für aktuelle Handys oder für EPC-Tags mit LL-Feature, Lizenzen zu beanspruchen. Alle Produkte sind neu und verletzen mit diesen neuen Features meine Patentansprüche. Ich hätte das wohl sogar auch nur mit dem Anspruch eines (neuen) selber verriegelbaren Microchips mit Internet-Nummer geltend machen können. (EPC-Tags an "Cola" Dosen nicht (ausser die neuen der nächsten Generation, die wohl nie mehr kommt, weil die jetzige schon die letzte und beste ist), dafür (neu) bei EPC-Tags in Hosen aus Datenschutz- und Autorisations-Gründen etc. ja.) Nur hätte ich ein paar Features weniger beanspruchen können im Gegensatz zur (absichtlich wie auch unabsichtlich) selber verriegelbaren Öse mit Nummer im Internet.

Sicher fallen ja selbst die aktuellen Handys unter mein Patent, welche man dann zur legal machbaren Lokalisation aus Datenschutz- und Autorisations-Gründen (selber) verriegeln kann. Solch ein Feature gab bzw. gibt es nämlich noch nicht bei den Handys! Trotzdem für das WAP-Handy kann ich keine Lizenzen verlangen, weil es schon existierte, bevor ich meine Erfindung machte. Aber ich kann Lizenzen verlangen, sobald man es selber mit all den Lock-Loop Funktionen verriegeln kann.

Ganz sicher: Der Theft Guard von Phoenix verriegelt Laptops, weswegen diese Laptop Hersteller mir Lizenzgebühren bezahlen müssen. Das ist das genau gleiche, wie bei den Handys und den EPC-Tags, wo ich für deren selber ausführbaren Verriegelung (aus Datenschutz- und Autorisationsgründen) das Schutzrecht beanspruche. EPC-Tags selber verriegeln aus Datenschutzgründen gab es noch nie!

PAGE INTENTIONALLY LEFT BLANK

... last but not least falls ein anderer Erfinder solch ein Patent schon angemeldet hat, soll er das auch erst durchsetzen, bzw. Intel bzw. IBM und allen andern Laptop-Herstellern etc. dieses Patent finden und gegen mich auslegen. Sowieso ist dieses Feature "Sender im Laptop" ein anderes Feature als "Öse mit Sender auf eine Nummer im Internet". Also müssen Laptop-Hersteller sowohl mir, als auch dem anderen Erfinder Lizenzen bezahlen. Leider verletzen die (PCMCIA-Slots) Steckkarten nicht meine Erfindung, weil sie keine fest installierten Sender sind und weil sie schon bekannt sind und somit Stand der Technik sind. Aber das hat mich umso mehr überzeugt, dass Centrino Laptops meinen Patentschutz verletzen (werden).

Und glauben sie mir, dass ich mit der Ösen-Internet-Nummer nicht nur ein Diebstahl-Sicherheits-system zum Patent angemeldet habe. Wenn man alle Ansprüche in der Anmeldung nun betrachtet, sieht man unendlich viele Funktionen (verriegeln, blockieren, verbinden, informieren, ausführen, managen...) für Handys wie auch für Laptops. Deswegen gilt das Gegen-Argument nicht, dass Centrino Laptops ja gar kein DSS hätten, um meinen Ösen-Internet-Nummer Sende Anspruch zu entkräften. Sowieso werden in Zukunft alle Laptops auch den Theft Guard haben und dann auch diese DSS Lock-Feature zusätzlich verletzen. Uff1

Im schlimmsten Fall kann ich sogar noch eine richtige "sophistische" Wortverdreherei machen, um meine hier formulierten Geltendmachungen zu untermauern. Die ersten beiden Linien in meinem 1. Patentanspruch lauten: Diebstahlsicherheitssystem einer mit einem Schloss verriegelbaren Öse oder mit mehreren Schlössern eine oder mehrere verriegelbare Ösen, ...(die als Einheit eine im Internet registrierte Nummer...trägt)! Diebstahlsicherheitssystem nervt mich enorm, dass mein Patentanwalt, Herr Spierenburg das so zu formulieren zuliess. Nun aber, ich kann auch sehr gut damit leben, weil unendlich viele Funktionen bei Laptops nur um das gehen, dass nicht Informationen gestohlen werden bzw. nicht weg kommen. Uff2. Transistoren bzw. eben Mikrochips sind ja nichts anderes als schliess bzw. verriegelbare und aufmachbare Stromkreise bzw. Ösen. Also schliesst bzw. verriegelt der Transistor im Chip wie ein Schloss Stromkreise bzw. Ösen genau so, wie ich es in den ersten beiden Linien meines ersten Anspruches formuliert hatte. Uff3. Kein wunder hatte ich so gejubelt, als mir das mit den Chips klar wurde, dass diese Chips ja selber im wahrsten Sinne des Wortes aus Ösen (Stromkreise) und Schlössern (Transistoren) bestehen und dazu noch gerade selber das Signal zur Nummer im Internet senden konnten und auch gleich noch die noch Nummer in sich wortwörtlich tragen! Uff3

Ich hoffe, Sie pflichten meinen Erklärungen bei und finden auch, dass mein Ösen-Internet-Nummer Funk-Feature für Laptops ich erfunden habe. Damit ist aber noch nicht ganz geklärt, ob es auch erfinderisch sei, weil eben WAP-Handys das selbe Ösen-Internet-Nummer Funk-Feature auch schon besassen. Das ist bzw. war aber für Handys, welche (bei den Ösen) mit den selben Molekülen, Wellen und Frequenzen funktioniert wie Laptops. So etwas mit selben Molekülen, Wellen und Frequenzen (auch bei den Ösen) kann man nicht erfinden bzw. ist nicht erfinderisch. Es (mit auch bei den Ösen) muss für ein anderes Feature bzw. mit einer anderen Merkmalskombination erfunden werden, damit es erfinderisch ist. Laptops sind/haben ein anderes Feature bzw. eine andere Merkmalskombination als mit/bei Handys, nur schon, weil sie einen anderen Namen haben als auch nicht direkt ins Internet funken konnten (kein WAP, kein GSM- oder (W-LAN) Transponder oder keine Antenne hatten), und mit einigen anderen Funktionen ausgestattet sind, weswegen es nur schon deswegen erfinderisch ist. QED2. Uff4!

N.B. das erste Handy mit wie bei Centrino Laptops selbem W-LAN Feature kam erst Anfang 2003 von Motorola heraus. Motorola müsste mir doch auch Lizenzen bezahlen? Ja, weil dieses neue Feature noch nicht bei den anderen Handys existierte aber ich es zuvor neu erfand. Das ist genau das Selbe, wie ich es oben mit den Handys der 4. MFG schon zur Neuheit geschrieben hatte. Damit müssen wirklich alle neuen Produkte (sogar auch ohne Funk- oder Verriegelungs-Feature), die eine Öse mit Nummer im Internet haben mir Lizenzen bezahlen, wie ich es patentiert und bzw. immer wieder schon gesagt hatte. Uff5. Die dazu notwendige Berechnung-Logistik ist kindereinfach. Jedes Produkt bekommt einen EPC-Tag und für diesen müssen mir Lizenzen bezahlt werden.

wird das Lock-Loop Patent (wie jedes) in zwei Kategorien unterteilt und so umschrieben mit folgenden von uns (neu) festgehaltenen Merkmalen:

Vorrichtung:
-Öse (Chip) mit Nummer (mit weiteren Informationen)
-Nummer in Datenbank (Internet u. über Mobiltelefon für jedermann zugänglich, etc.)
-Öse selber verriegelbar und aufmachbar (mechanisch, elektronisch, örtlich, zeitlich, rechtlich oder einer Kombination davon etc.)
-Nummer sichtbar (im Internet, auf Handy-Display oder Produkt z.B. als Seriennummer)

Verfahren:
-Senden und Empfangen der Nummer (mit weiteren Informationen auch über einen Transponder, d.h. das Funk-Feature)
-Vergleich der (Osen) Nummer und Informationen mit Datenbank (Nummer)
-Falls Nummer (zerstört wird oder) in Datenbank gekennzeichnet: Alarmsignal (oder Verriegelung der Öse, d.h. Lock-Loop Feature oder andere Funktion wie Tracken der Öse über GSM, GPS oder normalem Funk)

Nur falls jemand ein gleiches Patent mit den selben Funk- oder gar LL-Feature z.B. für WAP-Handys und alle anderen Produkte angemeldet hat, wäre bei Laptops dieses Patent schon an jemanden anderen vergeben. Andererseits bei Laptops kann das Funk-Feature als auch das LL-Feature nicht als Stand der Technik bezeichnet werden. Natürlich könnte wieder jemand das Funk-Feature etc. nur für Laptops angemeldet haben. Dann könnte es sogar sein, dass die Laptop-Hersteller durchaus zwei, drei Mal Lizenzen bezahlen müssen für ähnliche, sogar Diebstahlsicherheitssysteme, aber leicht verschiedene Funktionen.

Man kann mir keinen Vorwurf machen, nicht genannt zu haben, für welche Produkte mein Patent Verwendung finden kann. Einerseits habe ich eine ganze Palette von Produkten aufgezählt, andererseits kann ich nicht wissen, in welchen Produkten noch alles meine von mir erfundenen Features und Funktionen eingebaut werden bzw. welche Produkte noch keinen solchen Patentschutz hätten, wie scheinbar die Laptops. Z.B. wusste ich auch nicht, dass EPC-Tags zur Verriegelung keinen Patentschutz hatten.

Natürlich ist meine Erfindung ungemein breit und ev. letztlich doch sogar auch noch WAP-Handys müssten hier hinein fallen, weil ich das erste Mal an die Ösen-Internet-Nummer Erfindung schon etwa 1998 dachte und schon sogar damals in einer meiner anderen Patentanmeldungen beschrieb, wo

noch gar keine WAP-Handys vermarktet wurden. Hmm, WAP-Handys hat wohl auch niemand patentiert... aber von denen kann ich sowieso nicht mehr lange Lizenzgebühren verlangen.

Zudem gibt es (noch) keine Handys, welche man (selber) verriegeln kann und gleichzeitig über die GSM-Netze tracken kann. Man kann zwar bei den Einstellungen das Handy (nicht nur die SIM-Karte) blockieren lassen, wenn der PIN-Code drei Mal falsch eingegeben wird, aber wie bei Laptops bleibt dann das Gerät weg, weil es noch nicht trackbar ist!

Ein Patentanwalt hat mich auch noch auf gewisse Eventualitäten aufmerksam machen wollen, dass ev. jemand anderes dieses Patent auch schon angemeldet hätte bzw. doch sicher die Industrie. Wie früher schon geschrieben, kennt Phoenix Technologies, Intel, Swisscom Mobile und IBM Schweiz nichts dergleichen. Intel hat kein solches Interesse für die Laptop-Hersteller ein Patent anzumelden bzw. als dass sie es wohl auch vergessen bzw. übersehen hatten, ein solches einzureichen und mitzuverkaufen zur Centrino-Funktion, weil Intel nur Chips aber keine Laptops herstellt. Die Laptop-Hersteller haben selber auch gar nicht daran gedacht, das zu patentieren, als sie die Centrino-Funktion zum Kauf und der Integration offeriert erhielten, als dass ich dann schon meine Erfindung gemacht und eingereicht hatte.

PAGE INTENTIONALLY LEFT BLANK

Unterteil zusammenfügbar bzw. befestigbar ist (Motoren können nicht mehr an das (oder vom) Chassi (ab)gehängt werden), wobei eine Öse (Englisch: loop) ein Materie- oder Informations-Kreis auch über Licht-schranken oder Magnet- oder Elektro-Potential Felder hinweg ist und auch örtliche, zeitliche oder rechtliche etc. Ösen-Bereiche bzw. -Gebiete bzw. Kombinationen hiervon meint.

2. Der Alarm wird bei Zerstörung der Öse als auch bei Unterbruch der Speisung des Transponders (der Handy SIM-Karte) bzw. eines Speisungsmessers getätigt.

3. Die Öse hat eine grelle Leucht-Farben-Lackierung! Die Nummer auf der Öse wird mit einem 1 mm oder 0.5 oder 0.3 oder 0.1 oder 0.05 oder 0.03 oder 0.001 mm Laser eingraviert (durchgehend oder auch nicht) oder wird durch ein Lock-Loop (TM, Trade-Mark) Zeichen klar erkennbar gekennzeichnet!

4. Die Öse kann mit (einer Schraube und/oder Mutter, mit) einem Schloss, mit einer Öse oder Schloss selber verriegelt oder geöffnet werden, bzw. seriell oder parallel verriegelt/verschlüsselt/codiert und/oder kombiniert angeordnet werden.

5. Das Schloss kann durch, an, in, bei, für, anstelle der Öse und vice-versa umgekehrt befestigt und/oder verwendet werden. Die Nummer kann selber verriegelt, verschlüsselt, blockiert oder unsichtbar gemacht werden.

6. Die Befestigung des Lock-Loop DSS an die verschiedenen Produkte mit Schrauben, Nieten, Kabeln etc. geschieht immer mit einem quadratischen 4x4-oder 3D-Verbindungssystem mit 1 cm, 2 cm etc. Seitenabstand!

7. Die Nummern, die Ösen die Transponder sind alle einer technischen, wirtschaftlichen oder sonstigen Unterteilung wie Nomenklatur unterworfen, so dass sie sich nicht in die Quere kommen, sich überschneiden oder gegenseitig beeinträchtigen.

8. Vorrichtung bei der an einem Ober- und/oder Unterteil mindestens eine Öse vorgesehen ist, welche als Diebstahlschutz von einem Schloss derart verriegelt werden kann, dass der Oberteil nicht mehr mit dem Unterteil

PAGE INTENTIONALLY LEFT BLANK

14. In GSM-, UMTS- funkfreien Zonen (Tiefgaragen, Tunnels, Gebirge, Städten, Wäldern) können W-LAN (Accesspoint), Bluetooth, Wireless(local)loop oder CB-Funk Netze die Abdeckung übernehmen für die Funk-Interface, die auch verriegelt werden und ein Alarm auslösen lokal oder auf eine Zentrale oder ein Mobile Phone.

15. Die für den (GPS-, GSM- etc.) Funkempfang nötige Antenne ist in der Öse integriert und kann innen oder aussen am mobilen oder immobilen Objekt sichtbar oder unsichtbar, versteckt oder gekennzeichnet nicht (zerstörbar) oder zerstörbar angebracht sein und in die Öse oder Nummer integriert sein!

16. Die Funk-Interface haben mehrere Ösen bzw. eine Öse hat mehrere Funk-Interfaces, welche so angeordnet es (nicht mehr und) möglich macht, exakt definierbare elektrische Strom bzw. Schaltkreise einzurichten. Es kann (nicht mit einer Technik) gesagt werden, wie viele und was für welche Funk-Interfaces integriert sind! Das Selbe gilt für die Speisung.

17. Die Anordnung der Nummer, des Schlosses und der Ösen, Senders u. Chips kann so leicht gebaut und gestaltet werden, dass sie zwar ohne Beschädigung auf Jahre hinaus funktionieren, aber bei geringfügigen Verletzungen zerstört werden bzw. ein Alarm los geht. Die Öse, die Nummer, der elektrische Schaltkreis kann so auch eine Einheit mit der Nummer als z.B. einem Zifferblatt bilden. Das Schloss kann selber eine solche Einheit bilden, wie jede andere Anordnung mit einer Öse z.B. Schrauben, Muttern, Nägel, Nadeln, Fäden, Knöpfe, Stift, Niete, Ring, Platte, Kugel oder Box mit Öse und Nummer.

18. Im Fall des Schlosses bzw. einer Kugel oder Box kann diese noch zusätzlich mit einem normalen Schlüssel-System mit oder ohne Funkübermittlung (elektronisch) verriegelt werden. Aus dem Schloss, insbesondere der Kugel oder Box treten dann Kabel oder Schlaufen als Ösen, welche innerhalb von der Kugel oder Box einen geschützten Transponder, Transmitter bzw. Sender besitzt. Die Box oder Kugel kann selber aus mehreren Ösen gebildet bzw. damit geschützt sein!

19. Die einzelnen Kabel bzw. Ösen mit Isolierungen um den Draht können so verdrillt bzw. verwoben (wie ein Koaxialkabel) werden, sodass zwischen Austritt

und Eintritt der Kabel beim Sender bzw. der Sicherheitsbox kein Zugriff auf das selbe Kabel mehr möglich ist zum Kurzschliessen des selben. Der Sender kann sogar innerhalb des verwobenen Kabels integriert sein und die einzelnen Kabel können Antennen sein.

20. Die Verriegelung der Ösen und Nummern kann für Monitore und Radio-, TV-, W-LAN-, Telefon- etc. Empfänger und Sender verwendet werden, welche andere oder gleiche verschlüsselte und unverschlüsselte Signale empfangen oder senden. Die Signale können getrennt einzeln oder zusammen oder in einer Kombination davon übertragen werden!

21. Der elektrische Stromkreis in der Öse kann auch zusammen mit oder ohne der Öse geöffnet werden, um andere Ösen und Stromkreise hineinzulegen oder einen Zugang zu einem verriegelten Teil bzw. einer Box oder durch einen Durchgang wie (Auto-) Türen etc. zu ermöglichen.

22. Die Code-Verschlüsselung kann über einen externen oder internen, aktiv einschaltbaren oder passiv immer eingeschalteten Algorithmus mit einer speziellen Software auf einer speziellen Hardware geschehen.

23. Es können vom Transponder in Produkten auch einfach (elektronische) Verbindungen (Loops) zu den Peripherieteilen mit oder ohne Nummern gehen. So z.B. bei Computern bzw. Laptops können alle Peripherie-Teile (Laufwerke, Steckkarten, Chips, Kühlgeräte) erfasst werden und auf Komplettheit und/oder Anwesenheit geprüft werden. Hierzu kann auch die Microsoft PIN-Identifikations-Lösunge verwendet werden.

24. Neben dem Internet selber, können auch Funk-Interfaces und –Devices, Handys oder mobile wie stationäre W-LAN etc. oder RFID Transpondergeräte die Nummern speichern und verwalten.

25. Die Öse mit der Nummer kann neben dem elektrischen Stromkreis auch nur ein Informations-(Strom)kreis (z.B. die Verriegelung, ein Code, ein Signal oder eben eine Information) sein, der z.B. neben Materie als Träger über Licht, Ton, einem anderen physikalischen oder parapsychologischen Medium eine Information beinhaltet. Z.B. jede Lichtschranke kann mit einem Licht-

Wellenlängen-Code verriegelt werden oder jedes Magnet- oder Elektro-Potential-Feld kann auch Ösen bilden.

26. W-LAN, GSM etc. Transponder können RFID EPC-Tag Signale empfangen. RFID EPC-Tags empfangen und senden im W-LAN Frequenzbereich und können mechanisch, elektronisch, örtlich, zeitlich, rechtlich etc. oder in einer Kombination davon verriegelt werden mit einem Verschlüsslungsalgorithmus und haben eine Tracking- bzw. Registrierungs-Funktion mit Nummer im Internet.

Handy mit EPC-Transponder und Fingerprint-Sensor:

27. Der verschlüsselte Code (Firewall) kann aus einem biometrischen (Pin, Finger-Print, Akustik-Signal, Iris-Print) Code oder einer Kombination davon übertragen werden. Die Erkennung kann vice-versa rückgekoppelt sein.

28. Der biometrische Code zur Verriegelung der Ösen bzw. Nummern kann über ein Autoschlüssel (Zentral-Verriegelung), Mobil-Telefon, oder sonstigem Transponder gesendet werden, welcher für die Fingerprint Erkennung einen Sensor-Pad trägt und für die Iris-Erkennung eine Sensor-Kamera besitzt.

29. Die Sensor-Kamera sucht ein oder die beiden Schwarzen Pupillen und weissen Augäpfel mit Iris oder einen angebrachten oder integrierten EPC-Tag im Gesicht, Auge, Netzhaut, Hornhaut oder Linse, welche mit mindestens einem EPC-Tag auf das Auge gelegt wird. Die EPC-Tags können in die Augen operiert bzw. gelasert werden. Die EPC-Tags können direkt Video-Bilder auf die Linse projezieren, bzw. Richtungen anzeigen, welche in den Gelben Punkt des Auges gerichtet werden.

30. Kameras in Handys haben einen Sensor mit Software, die einen bei Video-Telephon-Gesprächen den Head-Set oder einen anderen Bezugspunkt immer das Gesicht, Körper oder einen anderen gewünschten Blickwinkel (z.B. auf einen speziellen EPC-Tag als auch mit Nummer im Internet) wie ein bewegliches Auge selber zentriert.

31. Die Verriegelung/Verschlüsselung der Öse und/oder Schlosses wird über ein Funksignal (GSM, CB, FM, IR, UV UHF etc.) getätigt! Dabei wird dem Produkt über ein Interface (Handy mit RFID Transponder, Schlüssel etc.) ein Zertifizierungscode verschickt. Das Funk Interface, d.h. Handy ist bzw. und hat selber wie das Produkt die oder eine, zweite, dritte etc. Öse mit Nummer. Auf dem Interface kann wiederum ein weiteres Interface als (Öse) angebracht und verschlüsselt werden, mit und ohne, dass das erste Funk Interface eine verriegelbare Öse ist bzw. verwendet wird. (Z.B. Schlüssel kombiniert mit Mobile Phone). Es können alle Interface und Produkte oder nur Teile davon kombiniert und individuell oder algorithmisch vorgegeben eingestellt werden. Vom Schlüssel kann ein Signal auf das Mobile Phone oder umgekehrt gegeben werden, welches nach einem vorgegebenen Algorithmus bedient werden muss oder kann!

32. Das Look-Loop DSS bzw. der Chip mit der Öse kann mit einem Lawinensuchgerät in Handys oder einer anderen Radar Suchfunktion bzw. Richtungsanzeige-Technik zu EPC-Tags, GSM-Chip oder GPS-Sender, Recco-Reflektor und -Sender etc. ausgestattet bzw. kombiniert werden z.B. in Handies, Skis, Snowboards, Bindungen, Boots oder Kleider oder allen andern Produkten.

33. Produkte (Funk-Interface) mit dem Lock-Loop DSS Feature können über W-LAN-, GSM-, GPS oder alle anderen Funk- Chips (CB, Walki-Talki 446000 MHz, Barryfox 457 kHz) senden. Die einzelnen Kanäle können wiederum verriegelt und verschlüsselt sein. Es sollen Handys, Walki-Talki etc. zu Multi-Funk (Sende- und Empfang-, bzw. Lokalisations- und Verriegelungs-) Einheiten verschmolzen werden. Dabei kann jede Kombination von Sende/Empfangs Einheiten gewählt werden, sei das UHF, GSM, Bluetooth, Sateliten-Telefon, GPS, DECT Festnetztelefonie.

34. (Funk-Interface) haben sowohl eine Hardware- als auch eine Software Lösung für die Einstellung der billigsten oder besten oder individuell gewünschten Reihenfolge der geeignetsten Abklärung der Uebermittlung der Verriegelung, des Codes, einer Such-Funktion als auch eines Gespräches sei über das UHF, GSM, Bluetooth, Sateliten-Telefon, GPS, DECT oder Festnetztelefonie. Mehre

PAGE INTENTIONALLY LEFT BLANK

PAGE INTENTIONALLY LEFT BLANK

mehrere EPC-Tags eingebaut oder versteckt (z.B. im Motor etc.). Aber neben Türen können auch Fenster, Cabriolet-Verdeckungen, Anhänger etc. oder sonstige Teile und Produkte verriegelt und getrackt werden.

44. Die Lock-Loop DSS Stand-Alone-Device in Fahrzeugen oder allen anderen Produkten senden, solange sie nicht gestohlen werden. Danach wird nur nach der Autorisation des Besitzers die Device kurze Signale geben, damit die Diebe die Device nicht suchen und zerstören können. Bei Verriegelung registrieren die Devices den Ort durch Positionierungen zu den GSM-, GPS- und anderen Sendern und falls eine unerlaubte Verschiebung oder Unterbrechung eines Loops passiert, wird ein Alarmsignal ausgesendet.

45. Auch ohne Funk Device genügen die EPC-Tags in den Fahrzeugen, um bei unerlaubter Zerstörung des Loops oder Verschiebung aus dem definierten Funkbereich über eine andere Funk Device in einem anderen Fahrzeug oder am Strassenrand oder über ein fremdes Handy etc. ein Alarm-Signal auszulösen.

46. Kombination eines Vorganges für ein Gerät wie Handy, PDA oder Laptop, welches gleichzeitig bzw. hintereinander unabhängig voneinander nachfolgend Biometrie, Finger-Print und Spracherkennung oder Nummern bzw. weiterer individueller, persönlicher Schlüssel Code oder Passwort Autorisation für eine Funktion "Auto verriegeln, öffen" etc. hat. Dieser Befehl wird über einen RFID Sender in einem Funk-Interface bzw. Handy auf die EPC-Tags gesendet.

47. Eine Software in den Lock-Loop DSS Stand-Alone-Device regelt und speichert alle empfangenen Signale von den umliegenden EPC-Tags. Durch mehrfaches Verriegeln aller EPC-Tags können diese zusammengenommen werden, die so ein einzelnes Produkt definieren. Durch eine Homoligisierungs-Funktion können weitere EPC-Tags hinzugenommen oder weggenommen werden.

48. Für Fahrräder wird eine doppelte oder dreifach Spange mit Ösen an den Rahmen befestigt, die in den Rahmen oder andere Bestandteile integriert werden können, welche selber Ösen oder Schlösser sein können (Z.B. Naben,

Achsen, Felgen, Sattel, Lenker, Griffe, Bremsen, Pneu). Insbesondere können Naben-Schlösser mit dem Diebstahlsicherheits-System ausgestattet sein!

49. Bekannte Fahrrad-Schlösser (Gabel-, Ketten- oder Kabelschlösser) haben einen GSM-, GPS oder EPC-Tag Transponder integriert zur Lokalisation und zur elektronischen Verriegelung des Schlosses. Für Fahrräder oder anderen nicht mit Strom gespiesene Schlösser und Produkte ist die Stromversorgung in die Nabe oder Felge als Bewegungsdynamo integriert oder eine Magnetscheibe (z.B. in der Scheibenbremse) im Rad als Induktions-stromerzeugung. Ein Bewegungssensor schlägt Alarm beim Wegtragen des Fahrrades oder bei Zerstörung. Bei Stromunterbruch oder Entwendung gibt es einen Alarm. Bei unerlaubter Entfernung von EPC-Tag bestückten Bestandteilen, wie Sattel, Rad, Bremse etc. gibt es auch einen Alarm. Jeder GSM-, GPS oder EPC-Tag Transponder kann individuell für ein Produkt kombiniert über die Fingerprint-Sensoren Funk-Interface oder das Internet verriegelt und getrackt werden.

50. Für die mobilen (Fahrzeuge (Stand-Alone-Lösung), Fahrräder, Laptops, Beamer etc.) Produkte wird die Funk-Antenne aussen oder innen ersichtlich oder unersichtlich oder versteckt angebracht. Die Hardware-Platine und die Transponder oder SIM-Karte als Empfangsmodul werden zusammen oder getrennt zwei-, bzw. mehrstufig über verschlüsselte Funk-Verbindungen mit der oder den Funk-Antennen verbunden. Die Transponder, SIM-Karte, Platinen und Funkantennen können selber miteinander verschlüsselt/verriegelt werden! Insbesondere kann in Produkte mit Funk- und Informations-Netzen zu Transponder zu EPC-Tags mit Transpondern zu GSM, W-LAN Netzen verbunden werden.

51. Auf einer (Lock-Loop DSS bzw. EPC-Tag Informations-) Internet-Plattform über Computer, Laptop-, PDA-, Handy- oder Funk Interfaces können alle anderen persönlichen, biometrischen, technischen etc. Daten eingegeben, verwaltet und verriegelt werden. Für Laptops, PDAs Handys und alle anderen Produkte mit LL Funk-Feature braucht es eine Lizenz von mir.

52. Zur (geschäftlichen) Betreibung der (Lock-Loop DSS bzw. EPC-Tag Informations-) Internet-Plattform etc., braucht es eine internationale Hotline für

die Fragen und Probleme der Kunden beantworten und lösen zu können. Verschiedene Organisationen und Institutionen können auch eingeschränkten Zugang zu der Internet-Plattform erhalten.

53. Das Lock-Loop DSS mit Transponder zu GSM-Netz und GPS-Sateliten und Transponder zu EPC-Tags kann als "Stand-Alone" Lösung direkt in (Auto)-Batterien, -Kabel-Bäumen, -Türen- oder -Zünd(Schlösser), oder Motoren integriert werden. Dabei wird die "Stand-Alone" Lösung vom Einbauer (Fahrer, Garagist) selber irgendwo mit einem oder mehreren Transpondern versteckt eingebaut. Die EPC-Tags konnen selber über Funk Daten und Informationen über Betrieb und Funktion übernehmen.

54. Für Fahrzeuge oder Laptops oder alle anderen ein- oder mehrteiligen Produkte mit einbaubaren Sender/Empfänger können weitere Tags (Microchips) als Lock-Loop DSS eingebaut werden in Motoren, Radios, Räder, Laufwerke, Mechanische oder Elektronische Bestandteile etc., damit diese nicht gestohlen oder ausgeschlachtet werden können. Hiefür können verschiedene Sender/Empfänger parallel oder seriell in die Produkte eingebaut werden. Insbesondere kann jeder Sender/Empfänger mit seiner Öse und Nummer verriegelt oder codiert werden und im Internet seine eigene Nummer besitzen, welche wiederum verriegelt oder codiert ist.

55. Bei Fahrzeugen melden die GSM-, GPS oder EPC-Tag Transponder alle Fahrzeugdaten (wie Tankstand, Abgaswerte etc.) den an den Strassen, Kreuzungen, Brücken, Tunnels bzw. Autobahneinfahrten, Zöllen etc., ob alles Korrekt ist. Autobahnfahrer und Polizei werden direkt informiert, falls ein Fahrzeug als Geisterfahrer auf die Autobahn gelangt. Im Nebel, Glatteis, Unfälle hinter unübersichtlichen Kurven, bei Unfällen und Staus etc., wird ein Signal den hinterherfolgenden Fahrzeugen übermittelt.

56. Fahrzeugstaus werden von Fahrzeug zu Fahrzeug rückwärts gemeldet und mit RFID Transpondern am Strassenrand (mit GPS etc. kombiniert) zur Stauauflösung gemanaged. Fahrziele können (akustisch etc.) eingegeben werden und über das Internet und einer Software zur Stauauflösung führen bzw. gar nie entstehen, weil ein solches höheres Verkehrsaufkommen sofort registriert und gemeldet würde. Eine RFID- etc. Black-Box registriert alle Bewegungen.

Ueber eine Schwerpunktsberechnung aus Fahrdaten der Fahrzeuge lässt sich von den Bremswegen über die Chache-Speicher die Höchstgeschwindigkeit und den Fahrzeugabstand bzw. gefährliche Fahrsituationen bei Baustellen in Nebel, Nässe und vor gefährlichen Kurven berechnen, bestimmen, melden oder gar aufzwingen. Verkehrsüberschreitungen können dem Fahrer mitgeteilt und v.a. rechtlich verbindlich nachgewiesen werden.

Sicherheit/Rechte/Spezial-Funktionen:

57. Die Funk-Interface bzw. Handys haben sowohl eine Verriegelungs- und/oder Such-Funktion nach Produkten mit bestimmten EPC-Tags mit Richtungsanzeiger etc., welcher auf eigene/fremde Produkte und/oder eigenes/fremdes Eigentum, neu/altem, billig/teuer, elektronisch/physikalisch, menschlich/animalisch/physisch Original/Fälschung einstellbar sind. Die Verriegelung kann auch von Handys (über das Internet) auf feste wie auch mobile Produkte, Türen etc. funktionieren.

58. Die Funk-Interface bzw. Handys erkennen die EPC-Tags, die in Marken-Label bzw. –Logos, im -Schriftzug oder dem -Zeichen oder nur der –Grundlage oder Preis- Barcode integriert sind, wobei diese mit weiteren Funktion wie nur Verriegeln zur Original-/Fälschungs- Erkennung einstellbar sind, d.h. das kann mit sonst irgend etwas wie mit Licht (Video), Ton (Music), Bewegung (Frische, Verpackung, Wärme, Zeit, Lagerung) von Konsumgüter und v.a. Lebensmitteln etc. mit EPC-Tags kombiniert werden. Jeder EPC-Tag wird über das Internet von einer von uns registrierten und gesicherten Site mit den Label-Listen geprüft, verriegelt und getrackt werden (können).

59. Die Funk-Netze sind auch Informations-Netze über EPC-Tags und Handy Funk-Interfaces. Die Funk-Interfaces (Antennen) können selber mit Funk verschlüsselt verbunden oder über Ösen verschlüsselt verbunden sein! Die Informationen der EPC-Tag-Netze können verriegelt werden oder/und zu weiteren Verwendungen von Individuen und Gesellschaften als auch Kolonien von Tieren, Menschen oder v.a. den Produkten selber herangezogen werden. Statistiken aus den Produkten und dem Netzbetrieb wie alle neu anfallenden

Informationen aus dem Zusammenhang mit dem Lock-Loop Projekt gehört dem Finder bzw. dem Erfinder!

60. Waffen, Wertgegenstände, Geräte-, Körper-, Fahrzeug- oder Flugzeug-Teil, Knöpfe, Reissverschlüsse, Bänder, Fäden können ein Lock-Loop- oder EPC-Tag-Chip beinhalten, der über ein Funk-Interface ein Signal auf eine Nummer im Internet gibt zur Kontrolle des Besitzers, Eigentum, Körperdaten, Verschleiss, Ablauf Rückgabe-Pflicht und Sperrung. Sinn und Zweck ist für die Gesellschaft und Individuen eine einfache Ueberprüfung aller verwendeter eigenen Rechte und fremder Pflichten zu ermöglichen.

61. Die Ösen können nicht nur für ein Produkt verriegelt/autorisiert werden, sondern auch für den Ort, einen Zeit-Punkt oder Spanne, einen Besitzer, ein Recht oder eine Pflicht (z.B. aus Datenschutzgründen).

62. Münzen, Geldscheine und Kreditkarten können ebenfalls mit einer (verriegelbaren) Öse, einem Microchip oder Transponder ausgestattet werden und mit zusätzlicher Information über Zeit, Ort, Vergangenheit, Besitzer gespeichert werden. Auf der verriegelbaren EPC-Kreditkarte sind alle persönlichen Daten abrufbar. Bei Zerstörung der Münzen, Geldscheine oder Kreditkarten können in einem Fall der ungewollten Zerstörung die Daten und Werte zurückgebracht werden oder im Fall der kriminellen Zerstörung werden die Daten und Werte blockiert bis zur offiziellen Abklärung. Die Münzen Geldscheine und Kreditkarten können so auch offiziell entwertet oder bewertet werden. Jede Transaktion jeder Münze und jedes Geldscheines kann in den Handys selber bzw. über das Internet verfolgt und nachgewiesen werden. Kein Falsch-Geld ist mehr möglich!

63. Die (Handy) Funk-Interfaces als auch Internet-Server haben ganz spezielle History-Caches, welche alle Transaktionen von EPC-Tags (Geld, Produkte) nach ganz verschiedenen Kriterien (Art, Zeit, Distanz, Menge, Kosten, individuelle Präferenzen) registriert, managed und anzeigt. Insbesondere kann jedermann seine transferierten EPC-Tags nachträglich nachverfolgen und überprüfen, auch wenn sein Handy ihm abhanden gekommen ist, übernehmen das die anderen Handys bzw. die Caches in den EPC-Tags selber, weil sie auch

für eine unbestimmte Anzahl Besitzer deren Nummern speichern bzw. verriegeln.

64. Die Nummer auf der Öse kann sichtbar oder unsichtbar physikalisch mit einer anderen Erkennungsmethode erkennbar gekennzeichnet werden und selber Öse sein oder die Öse eine Nummer, einen Informations-Teil oder -Ganzes kombiniert mit Funktionen, Codes, Aufgaben, Pflichten, Rechten, Bestimmungen sein.

65. Aus Umweltschutz- und Pfand-Gründen können alle Produkte beim Verkauf mit der Code-Nummer in der Öse zum Käufer und Besitzer in Beziehung gebracht werden. Bei der Entsorgung in (öffentlichen) Eimern, Depotstellen oder der Vernichtung können auch Sender jeden Öse (EPC-Tag registrieren). Daraus lassen sich ganze Stoffffluss- bzw. Logistik-Szenarios für Produkte, Marken, Firmen verwalten und vermarkten.

66. Die Produkte können über interne oder externe elektronische Verriegelungssysteme (so wie der Schlüssel zum Schloss eine Einheit bildet) gemanaged werden (die Ösen können ja verschiedene (einstellbare) Nummern besitzen). D.h. Handys, Fingerprint-Sensoren, Video-Kameras, welche eine Verriegelungs-, Autorisations- oder sonstige Funktion mit den anderen Produkten mit Ösen und Nummern haben, bilden eine Einheit oder können natürlich auch getrennt einzeln betrachtet, gebraucht oder verwendet werden. Z.B. Handys, Kameras, Tonbandgeräte können in Flugzeugen, Theatern, Konzerten, Vorträgen, Sportanlässen abgestellt werden.

67. In oder an allen privaten oder öffentlichen Gebäuden können RFID Identifikations-Sender angebracht werden, welche die EPC-Tags registrieren. So können permanent in Eingangshallen von Bahnhöfen oder an Autobahnen und an Flughafen Terminals Identifikations-Sender aufgestellt werden oder eben mobil über jedes Handy selber laufen.

68. Für Autorisationen von Internet-, Bank-, Eigentum-, Rechts- Zugriffen oder für Abstimmungen, Wahlen und dergleichen können die Lock-Loop DSS ausgestatteten und autorisierten Produkte verwendet werden.

69. Spezieller Knopf oder Funktion im Handy etc. lässt EPC-Tag, Produkt oder Freunde Information in 1 cm, 10 cm oder 1m etc. Distanz aufnehmen. Diese Information wird in einem Management Cache nach (Zeit, Länge, Ort, Index, Wichtigkeit, Merkmalen Wünschen) gespeichert. Spezieller Knopf oder Funktion im Handy, die das Radio- und TV-Kanäle und –Volumen vorlaufen zu lassen, Alarm auslösen oder einen Hochspannungs-Schlag (bei gewissen bzw. entsprechenden EPC-Tags) für Gefahren wie Allergien, Waffenbesitzer, oder bei gefährlichen Menschen, Tieren wie z.B. Hunden selber auslösen.

70. Beim Lock-Loop DSS können über Handy-, PDA-, Laptop-Interfaces spezielle Services eingestellt werden wie z.B. die Lokalisation von Freunden oder Feinden, sodass bei Annäherungen oder Entfernungen oder dem Verschwinden ein Alarm ausgelöst oder ein sonstiges Signal übermittelt wird z.B. beim Ueberschreiten eines verriegelten Elektro-Potential Feldes!

71. Die Verriegelungen/Autorisationen für die Ösen- bzw. EPC-Tags (Chips) können individuell oder für Gruppen oder Produkte eingestellt werden. (Z.B. kann für spezielle Werbung in Strassen, Malls, Busen, Trams, Zügen etc. nach individuellen Gesichtspunkten das Handy-Head-Set eingestellt werden oder es gibt einen Alarm, wenn ein Krimineller mit Waffe auftaucht, oder es werden Satelitengesteuerte etc. Wanderungen oder Touren durch (Produkte-) Parks möglich. Ein Knopf oder eine Funktion übernimmt die Handy bzw. Head-Set Einstellung auf TV-, Radio-, RFID-, Telefon oder Funk-Empfang.

72. Sofort-, bzw. moment Aufnahme Beweis mit Video- oder Foto-Aufnahmen (mit Blitz) und im Umkreis alle EPC-Tag Augenblick Speicherung, welche auch direkt mit Copy Right Schutz ins Internet mit der Nummer verriegelt werden. Das ergibt einen einfachen und genialen "Zeit-Zeugen"-, Authentizitäts- und Beweis- Standart.

73. Kombination von einem Handy (Funk-Interface) mit Stand-Alone-Lösung für Fahrzeuge oder EPC-Tracking und Verriegelung. Zusätzliche Funktionen wie Garagetüröffner, Fotoapparat etc. sind weiter integriert.

74. Alle (z.B. aus Datenschutz- und Autorisationsgründen) Ösen mit Nummern ohne Nummer im Internet sind (selber) verriegelbar oder auf einer Internet-

Site kann man alle seine verlorenen Produkte verriegeln lassen und zum Tracken ausschreiben mit Alarm und Meldefunktion an verschiedenste Parteien. Funk Interfaces (Handys) und alle GSM-, W-LAN Transponder werden weltweit alle Ösen und Nummern tracken.

75. Alle Ansprüche dieses Patentes werden mit den Ansprüchen meines Video-Hitlist Patentes kombiniert bzw. mit den Ansprüchen dieses Patentes selber kombiniert.

76. Jede Kombination jedes Patentes, Rechtes, mit diesem Patent oder mit dessen eigenen Ansprüchen, Beschreibungen, Sätzen, Wörtern ist (auch) möglich.

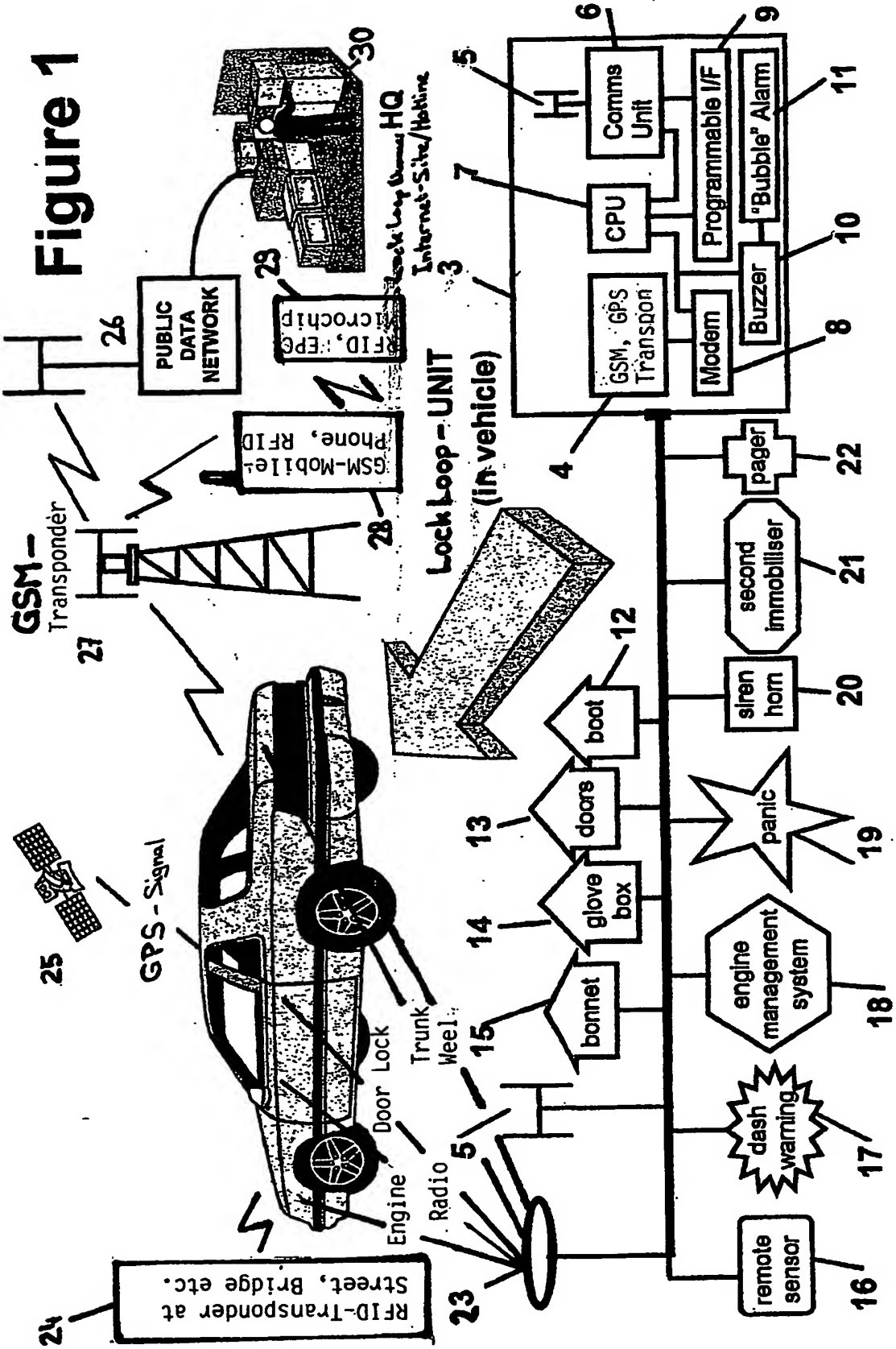
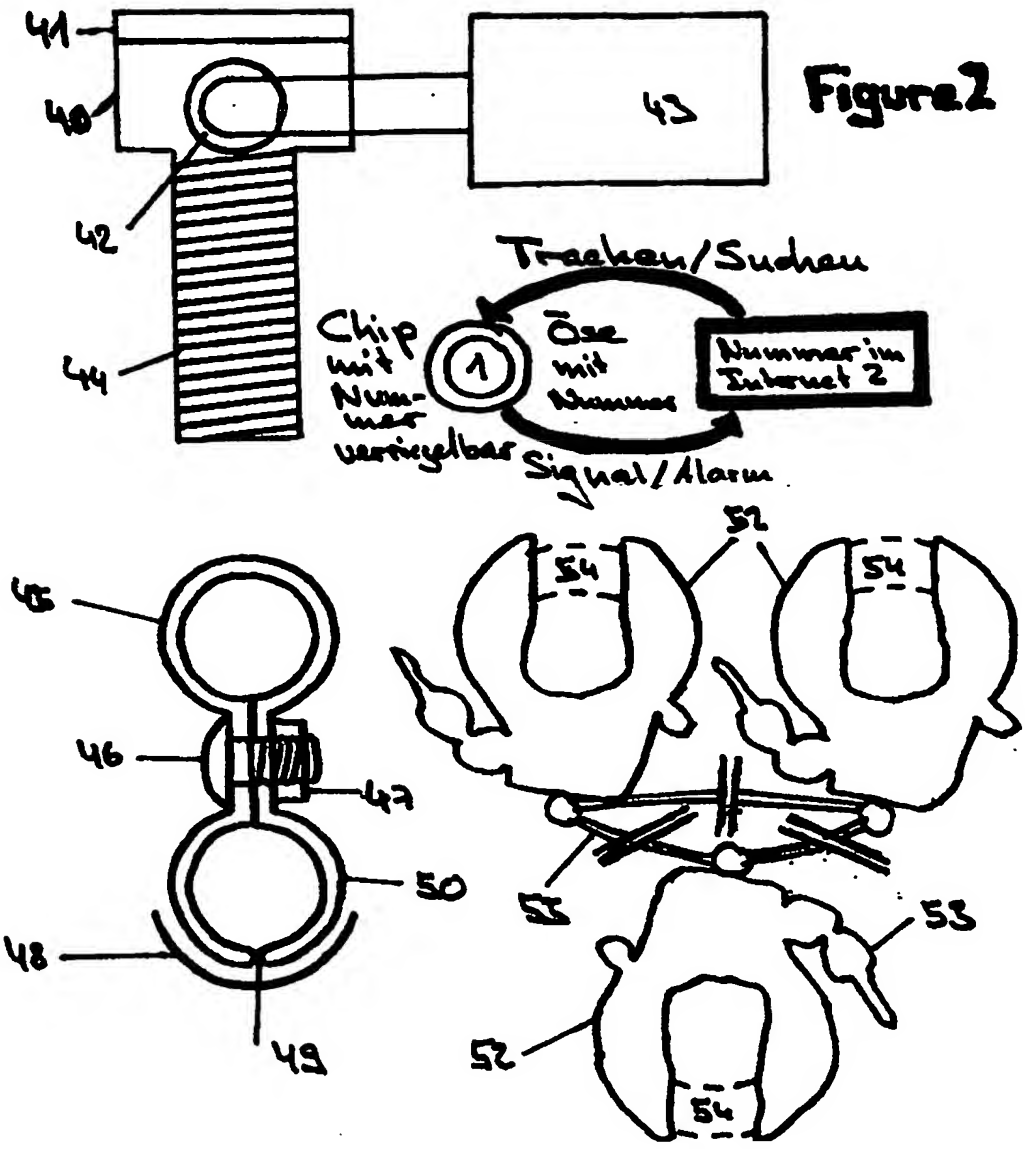


Figure 1
Lock Loop – UNIT (in vehicle)
GSM, GPS Transcon
CPU
Comms Unit
Programmable I/F
"Bubble" Alarm
Buzzer
Modem
pager
second immobiliser
siren horn
panic
engine management system
dash warning
remote sensor
boot
doors
glove box
bonnet
GSM-Transponder
PUBLIC DATA NETWORK
GSM-Mobile Phone, RFID
RFID, EPC Microchip
HQ Internet-Site/Hotline
GPS-Signal
RFID-Transponder at Street, Bridge etc.
Door Lock
Trunk
Wheel
Engine
Radio
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30


41
40
42
43
44
Figure2
Trachea/Sudan
Chip mit Nummer verriegelbar
Öse mit Nummer
Nummer im Internet ?
Signal/Alarm
45
46
47
48
49
50
51
52
53
54

Lock-Loop DCS

Figure 3

X = existierte noch nicht } kein Stand der Technik
□ = existierte schon } keine Publikationen
[X] = kommt ins ⊛ kommt realisiert (mein Pat.)